ных тестов; б) случайную, с возможным исключением для первого (для группы первых) и последнего (для группы последних) заданий, которые могут отбираться специально из соображений большей понятности, удобства, интереса и т.д.; в) специальную, в соответствии с какой-либо теорией, соображениями переноса навыков, концентрации внимания и др.; г) блочную, с возможностью выбора порядка подачи тестовых заданий в каждом блоке; д) в порядке, сочетающим случайный и специальный подбор. Существует довольно большое количество тестовых сред, однако нашей системе образования нужны надежные стандартизированные тестовые оболочки, а не любительские самоделки которые далеки от понимания тестологии контрольного материала.

- Балыкина Е. Н. Компьютерное дидактическое тестирование в преподавании исторических дисциплин // Круг идей: алгоритмы и технологии исторической информатики: тр. IX конф. Ассоциации «История и компьютер». – М; Барнаул, 2005. – С. 484–517.
- Концевой М.П. Тестовый комплекс в структуре электронного учебного пособия// Тезисы докладов Первой Международной научно-методической конференции «Перспективы развития системы тестирования в Республике Беларусь» 13 февраля 2003г. Минск: РИКЗ, 2003. С. 193-195.

Спиричева Н.Р., Любимцев С.И.
Spiricheva N.R., Lubimcev S.I.

ВЫБОР ПРОГРАММНЫХ ПРОДУКТОВ ДЛЯ ЛАБОРАТОРНОГО ПРАКТИКУМА ПО ДИСЦИПЛИНЕ “МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ”

CHOICE SOFTWARE FOR A LABORATORY WORK FOR DISCIPLINE “METHODS AND MEANS INFORMATION PROTECTION”

nr1382873@inbox.ru
ГОУ ВПО «Уральский государственный технический университет – УПИ имени первого Президента России Б.Н.Ельцина»
г. Екатеринбург

При формировании УМК по дисциплине “Методы и средства защиты компьютерной информации” был проведен анализ демонстрационных и свободнораспространяемых продуктов для использования в лабораторном практикуме.

At creation textbook for discipline “Methods means information protection” the analysis demonstration and open source products for use in a laboratory work has been carried out.

Для современного общества проблемы информационного обеспечения всех сфер деятельности являются первоочередными. Однако интенсификация информационных процессов порождает ряд попутных и достаточно серьез-

ных проблем, в том числе и проблему надежной защиты циркулирующей в системе информации.

Для формирования необходимых компетенций у студентов специальностей “Автоматизированные системы обработки информации и управления”, “Информационные системы и технологии” в указанной области знаний преподается дисциплина "Методы и средства защиты компьютерной информации". Основной проблемой в этой области подготовки студентов являются значительные материальные затраты, связанные с дорогостоящими программными продуктами и аппаратными средствами.

Альтернативный путь и единственно возможный при дистанционной технологии обучения – использование демо-версий дорогостоящего ПО и свободнораспространяемых продуктов. Для удобства и возможности самостоятельной работы студентов разработан электронный учебно-методический комплекс (УМК) “ Методы и средства защиты компьютерной информации ”, в состав которого включены рабочая программа дисциплины, конспект лекций, демонстрационное сопровождение лекционного материала и лабораторный практикум.

Лабораторный практикум имеет некоторую вариативную часть и пытается учесть интересы студентов в области защиты информации.

Лабораторная работа №1. Шифрование с открытым ключом. Система PGP. (PGP.com)

Лабораторная работа №2 (вариативная).

А) Самостоятельная реализация алгоритма криптографической защиты информации

Б) Криптографическая защита информации с помощью системы Крипто-Про (демо-версии http://www.CryptoPro.ru)

Лабораторная работа №3. Криптоанализ

Для демонстрации криптоанализа используются готовые программы, позволяющие открытие текстов, зашифрованных по алгоритму Вижинера. Студентам предложены следующие полезные ссылки:

I. Он-лайн программы для кодирования/декодирования текстов по алгоритму Виженера и анализа зашифрованного текста с неизвестным ключом.

1. По следующему адресу
http://math.ucsd.edu/~crypto/java/EARLYCIPHERS/Vigenere.html расположена программа, позволяющая проводить весь спектр операций, использующих алгоритм Виженера (рис.1):

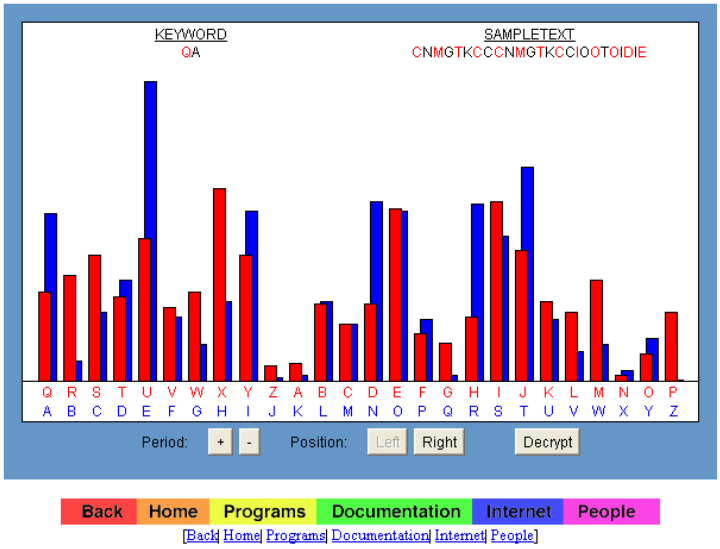

Рис. 1. Форма при проведении криптоанализа

Для работы сервиса необходим плагин *Java* для браузера.

2. http://sharkysoft.com/misc/vigenere/ Сервис, позволяющий только кодировать/декодировать тексты с помощью алгоритма Виженера и известного ключа.

3.http://smurfoncrack.com/pygenere/index.php Очень удобный сервис. Полностью автоматически анализирует зашифрованный текст, подбирает ключ и декодирует сообщение. Необходимо только задать интервал предполагаемой длины ключа.

II. Автономные программы для кодирования/декодирования текстов по алгоритму Виженера и анализа зашифрованного текста с неизвестным ключом.

1. Программа «Vigenere Cipher» http://pajhome.org.uk/crypt/vigenere.html. Написана на языке С. Осуществляет кодирование/декодирование по известному ключу и предоставляет широкие возможности по анализу текстов с неизвестным ключом.

2. Программа «The Vigenere Cipher», по функциональным возможностям идентичная предыдущей, находится по адресу http://mathdemos.gcsu.edu/mathdemos/vigenere/vigenere.html. Однако, в отличие от предыдущей, написана на языке *Visual Basic* и имеет графический удобный интерфейс.

3. Существуют даже программы для мобильных телефонов и коммуникаторов, позволяющие работать с алгоритмом Виженера. Вот одна для смартфонов на базе мобильной операционной системы Palm OS. http://www.palmblvd.com/software/pc/Vigenere-Cipher-2001-10-11-palm-pc.html

4. Следующая программа позволяет производить только кодирование/декодирование текстов по известному ключу. Однако к её достоинствам можно отнести дружелюбный графический интерфейс и форму установки в виде EXE-файла. http://www.brothersoft.com/vigenere-cipher-135713.html.

5. Мощнейший инструмент для анализа не только шифра Виженера, но и многих других. Официальный сайт программы http://www.cryptool.org/. Уди-

вительно, но при огромных функциональных возможностях – это бесплатный продукт и преподносится как *«свободный обучающий инструмент для криптографии и криптоанализа»*. Для примера рассмотрим, как с помощью данной программы зашифровать, а потом взломать зашифрованный текст. Для шифрования текста, который по умолчанию представлен в главном окне программы, пройдем по меню, как показано на рис.2.

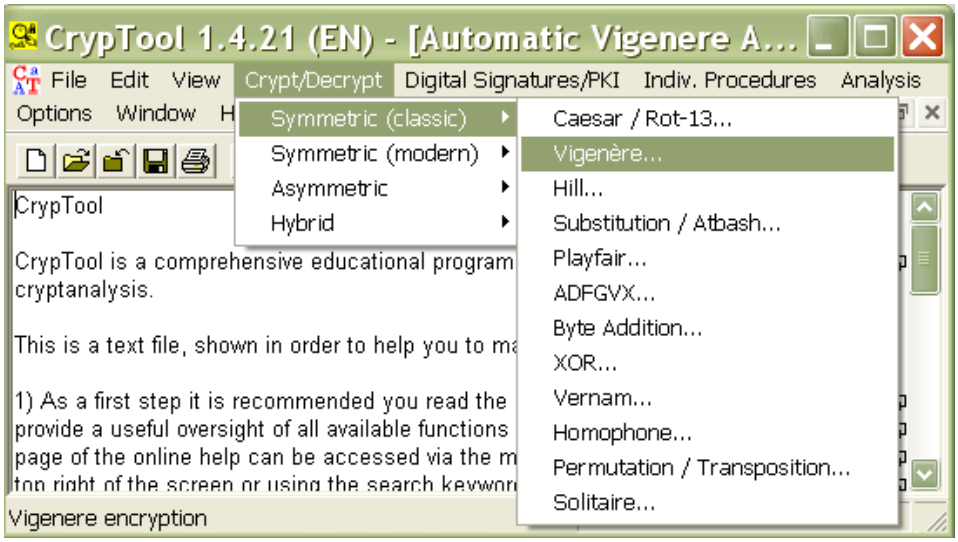

Рис.2. Шифрование текста

Появится окно для ввода ключа шифрования (рис 3). Введем ключ и нажмем кнопку *Encrypt*:

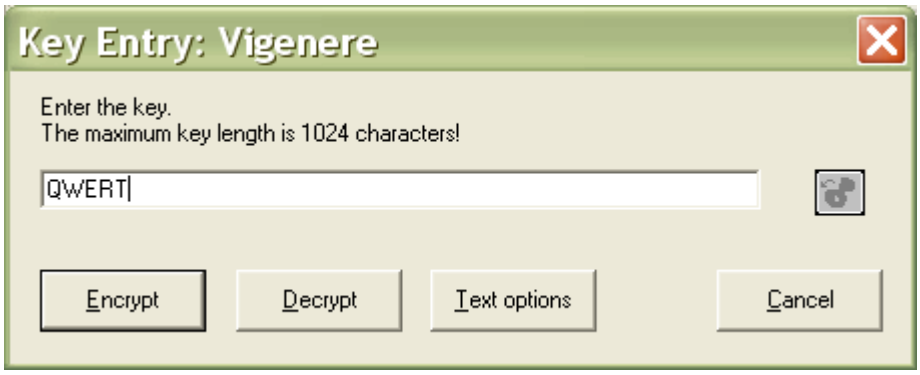

Рис. 3. Ввод ключа

Теперь текст зашифрован. Предположим, что мы забыли ключ, но нам срочно необходимо прочитать текст данного файла. Для криптоанализа проделаем действия, аналогичные представленным на рис.4.

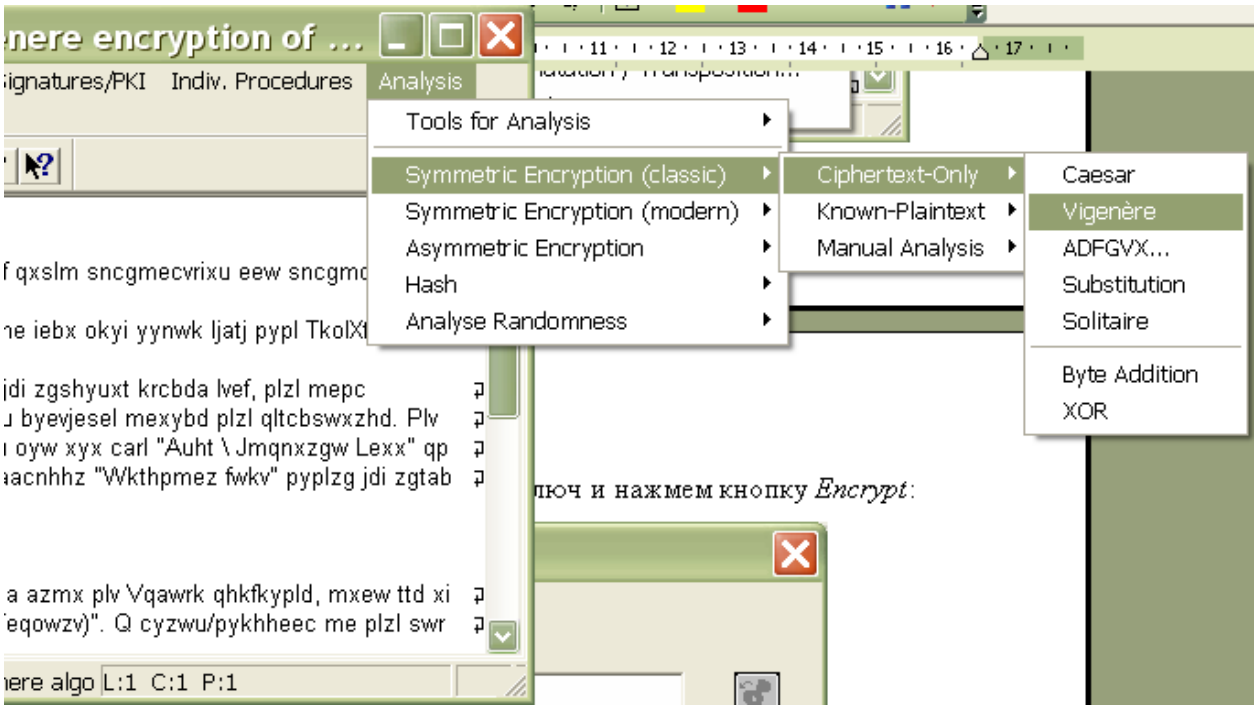

Рис. 4. Окно для криптоанализа

Программа попросит ввести длину анализируемого текста. Эта длина должна быть больше, чем длина предполагаемого пароля. Программа выведет ключевую последовательность, которая использовалась для шифрования исходного текста. Нажимаем кнопку *Decrypt*, и текст расшифрован.

Считаю, что знакомство с описанными программными продуктами сформирует необходимые компетенции у студентов в области программных средств защиты информации и криптографии.

Томашевский Д.Н.
Tomashevsky D.N.

МУЛЬТИМЕДИЙНЫЙ КОМПЛЕКТ УЧЕБНЫХ МАТЕРИАЛОВ ПО КУРСУ “СИЛОВАЯ ЭЛЕКТРОНИКА”
MULTIMEDIA TRAINING PACKAGE FOR THE COURSE OF LECTURES "POWER ELECTRONICS"

dnt0@mail.ru
ГОУ ВПО «Уральский государственный технический университет – УПИ имени первого Президента России Б.Н.Ельцина»
г. Екатеринбург

В статье рассматривается мультимедийный комплект учебных материалов по курсу “Силовая электроника”. Рассмотрены содержание, назначение, особенности представленных материалов.

In this article the multimedia training package for the course of lectures “Power electronics” is considered. The content, purpose, features of the presented materials are considered.

Для обучения студентов по специальностям 140605 “Электротехнологические установки и системы” и 140610 “Электрооборудование и электро-